ABSTRACT OF THE DISCLOSURE

When an electronic document is made available for review by other entities, it is often convenient to store the document in a repository or database managed by a third party. A system is provided in which the originator of the document is able to ensure the integrity and security of its document filed with a third party repository without having to trust the administrator of the repository. Both the document originator and the repository administrator have vault environments which are secure extensions of their respective work spaces. The vault of the document originator encrypts a document that it receives from the originator, prior to forwarding it on to the vault of the repository. On receipt of the encrypted document, the repository's vault signs the encrypted document itself before storing the document in the electronic repository and returning to the originator's vault proof of deposit of the encrypted document. When a request is made to view the document, it is made from the vault of the requesting party (a secure extension of the requesting party's work space) to the repository's vault. The repository's vault retrieves a copy of the encrypted document which it forwards, along with the requestor's identity to the originator's vault. The originator's vault verifies that the requestor is authorized to view the document from the access control list using an access control list identifying access ownership privileges for the document stored in the vault itself. If the requestor has access, the originator's vault decrypts the document and forwards the decrypted document directly to the requestor's vault. The requestor must provide proof of receipt of the decrypted document.